CIAware

Awareness Through Information Sharing

Incidents/Articles of Note:

- Turning Up The Heat: A Ransomware Attack On Critical Infrastructure Is a Nightmare Scenario
- White House announces ransomware task force — and hacking back is one option
- What Critical Infrastructure Providers Need to Do to Enhance Their Cybersecurity
- $10M for Info on State-Sponsored Attacks on US Critical Infrastructure
- 4 actions that can protect critical infrastructure from ransomware
- The Evolution of Securing Critical Infrastructure

TOOLS AND RESOURCES

To raise awareness of the risks to—and improve the cyber protection of—critical infrastructure, CISA and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory as well as updates to five alerts and advisories. These alerts and advisories contain information on historical cyber-intrusion campaigns that have targeted ICS:

- Joint CISA-FBI Cybersecurity Advisory (CSA): AA21-201A: Gas Pipeline Intrusion Campaign, 2011-2013 Note: CISA released the initial version of this publication to affected stakeholders in 2012.
- ICS Joint Security Awareness Report: JSAR-12-241-01B: Shamoon/DistTrack Malware (Update B)
- ICS Advisory: ICSA-14-178-01: ICS Focused Malware – Havex
- ICS Alert: ICS-ALERT-14-281-01E: Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
- ICS Alert: IR-ALERT-H-16-056-01: Cyber-Attack Against Ukrainian Critical Infrastructure
- Technical Alert: TA17-163A: CrashOverride Malware

CISA urges critical infrastructure owners and operators to review the publications listed above and apply the mitigations in Joint CISA-FBI CSA AA21-201A: Gas Pipeline Intrusion Campaign, 2011-2013. CISA also encourages owners and operators to review AR-17-20045: Enhanced Analysis of Malicious Cyber Activity. These products contain threat actor tactics, techniques, and procedures (TTPs); technical indicators; and forensic analysis that critical infrastructure owners and operators can use to reduce their organizations' exposure to cyber threats. Note: although these publications detail historical activity, the TTPs remain relevant to help network defenders protect against intrusions.

CISA encourages critical infrastructure owners and operators to report cyber incidents to CISA. Note: for information on the U.S. Department of State's reward program for identifying persons who participate in the malicious cyber activities against U.S. critical infrastructure, see the U.S. Department of State press release.

View Virginia Fusion Center Homepage

Click Here

Observe Suspicious Activity?

Report Online

Virginia Shield Coalition

"Awareness Through Information Sharing"

Need Help with this Email?

View in a browser

VFC Shield

"Awareness Through Information Sharing"

Useful Links

- VFC Fusion Site
- Shield Homepage
- All Products
- Report SAR
- Email Coordinator